Universidade Federal de Pernambuco

Curso de Sistemas de Informaação

Um Catálogo de Vulnerabilidades em Dispositivos IOT

Trabalho de Conclusão de Curso de Graduação

por

Thiago Conte Rocha

Orientador: Prof. Jéssyka Flavyanne Ferreira Vilela

Recife, Março / 2024

Thiago Conte Rocha

Um Catálogo de Vulnerabilidades em Dispositivos IOT

Monografia apresentada ao Curso de Sistemas de Informaação, como requisito parcial para a obtenção do Título de Bacharel em Sistemas de Informação, Centro de Informática da Universidade Federal de Pernambuco.

Orientador: Prof. Jéssyka Flavyanne Ferreira Vilela

Recife

2024

Agradecimentos

Eu gostaria de agradeçer a todos vocês que me ajudaram durante esta jornada, especialmente para:

Professora Jéssyka Vilela por toda mentoria e orientação durante todos esses meses.

Aos meus pais: Jairo e Miriam por sempre me apoiarem nos meus estudos.

Aos meus amigos: Thales Brederodes, Thiago Carvalho, Gustavo Nascimento, Thaís Conte, Liz, Pedro Novis, Victor Campelo, Breno Cruz, Daniel Lopes, Tiago Cardoso, Júlia Diniz e todos que fazem parte dessa enorme família.

Finalmente, eu gostaria de agradecer a toda a turma de SI 2019.2 É o começo do fim.

Trust me.

Qualquer tecnologia suficientemente avançada é indistinguível de magia.

Arthur C. Clarke

RESUMO

Com o avanço da Internet das Coisas (IoT), a segurança da informação em dispositivos conectados tornou-se uma preocupação crescente devido às vulnerabilidades exploradas por cibercriminosos. A falta de um catálogo abrangente de vulnerabilidades em dispositivos IoT dificulta a implementação de medidas eficazes de segurança cibernética para proteger esses dispositivos contra ameaças. Os objetivos desse estudo são identificar e catalogar as principais vulnerabilidades em dispositivos IoT, bem como analisar as soluções propostas na literatura para mitigar essas vulnerabilidades, visando fortalecer a segurança da informação nesse ambiente tecnológico em rápida evolução. Essa pesquisa foi conduzida em etapas, incluindo uma pesquisa inicial no Google Acadêmico, seguida pela técnica de snowballing para identificar novos estudos relevantes. Foram selecionados 12 artigos com critérios específicos de relevância e qualidade, abordando vulnerabilidades em dispositivos IoT e soluções para mitigá-las. A análise das vulnerabilidades em dispositivos IoT resultou na identificação de 26 vulnerabilidades comuns, como DDoS, Hijack Attack e Man-in-the-middle attack. Além disso, foram apresentadas soluções propostas para mitigar essas vulnerabilidades, contribuindo para o desenvolvimento de melhores práticas e estratégias de proteção. Ao destacar as vulnerabilidades mais prevalentes e as estratégias de mitigação propostas, este estudo reforça a importância de fortalecer a segurança da informação em dispositivos IoT. O catálogo elaborado fornece insights cruciais para promover um ambiente mais confiável e seguro para a utilização dessas tecnologias, destacando a relevância do snowballing como uma técnica eficaz na identificação de estudos complementares.

Palavras-chave: Vulnerabilidades, Segurança da Informação, Dispositivos IOT, Catálogo, Snowballing

ABSTRACT

With the advancement of the Internet of Things (IoT), information security on connected devices has become a growing concern due to vulnerabilities exploited by cybercriminals. The lack of a comprehensive catalog of vulnerabilities in IoT devices makes it difficult to implement effective cybersecurity measures to protect these devices against threats. The objectives of this study are to identify and catalog the main vulnerabilities in IoT devices, as well as analyze the solutions proposed in the literature to mitigate these vulnerabilities, aiming to strengthen information security in this rapidly evolving technological environment. This research was conducted in stages, including an initial search on Google Scholar, followed by snowballing to identify new relevant studies. 12 articles were selected with specific relevance and quality criteria, addressing vulnerabilities in IoT devices and solutions to mitigate them. Analysis of vulnerabilities in IoT devices resulted in the identification of 26 common vulnerabilities, such as DDoS, Hijack Attack and Man-in-the-middle attack. Furthermore, proposed solutions were presented to mitigate these vulnerabilities, contributing to the development of best practices and protection strategies. By highlighting the most prevalent vulnerabilities and proposed mitigation strategies, this study reinforces the importance of strengthening information security in IoT devices. The created catalog provides crucial insights to promote a more reliable and safe environment for the use of these technologies, highlighting the relevance of snowballing as an effective technique in identifying complementary studies.

Keywords: Vulnerabilities, Information Security, IOT Devices, Catalog, Snowballing.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

IoT	Internet of Things
CVE	Common Vulnerabilities and Exposures
UFPE	Universidade Federal de Pernambuco
CID	Confidencialidade, Integridade e Disponibilidade
DoS	Denial of Service
DDoS	Distributed Denial of Service
RFID	Radio Frequency Identification
RSSF	Rede de Sensores Sem Fio
RSN	Reactive Sensor Networks
GPS	Global Positioning System
WiFi	Wireless Fidelity
LTE	Long Term Evolution
OWASP	Open Web Application Security Project
TCC	Trabalho de Conclusão de Curso
SQL	Structured Query Language
GPS	Global Positioning System

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo são contextualizadas a adoção de dispositivos da Internet das Coisas, do inglês Internet of Things (IoT), a segurança das informações manipuladas por esses dispositivos, a motivação e a justificativa para este trabalho, respectivamente. Além disso, são citados os objetivos do trabalho, trabalhos relacionados são discutidos e a estrutura do trabalho é apresentada.

1.1 Contextualização

A Internet das Coisas (IoT) é um paradigma de comunicação emergente que visa conectar diferentes tipos de objetos à Internet, a fim de coletar dados gerados por sensores, controlar remotamente aparelhos e máquinas, monitorar ambientes, veículos e edifícios, e assim por diante. O número e a variedade de dispositivos IoT têm crescido rapidamente nos últimos anos, com uma previsão de mais de 50 bilhões de dispositivos conectados à Internet até 2020 [1].

Esse crescimento pode ser percebido através do notório aumento de acessos em diversas plataformas e redes sociais: Saber que, em 60 segundos, aconteceram em 3.8 Milhões de pesquisas no Google, 3.3 Milhões de Posts no Facebook, 29 Milhões de mensagens enviadas via Whatsapp, 448.800 Tweets no Twitter, 65.972 uploads de fotos no Instagram, 149.513 e-mails enviados, 500 horas de upload de vídeos no Youtube, e 1.440 posts no Wordpress [2]. O aumento no número desses dispositivos tem gerado dados alarmantes como: 98% de todo o tráfego de dispositivos IoT não é criptografado, 57% dos dispositivos IoT são vulneráveis a ataques de gravidade média ou alta [3].

Esses dados têm trazido preocupações com relação a segurança dessas tecnologias e dos usuários que as utilizam. Esses dispositivos têm variadas conexões com outros aparelhos a fim de tornar a sua rede interconectada, trazendo uma maior facilidade na integração entre eles e no uso para o qual foram projetados: de casas inteligentes até cidades inteligentes. Contudo, essa interconexão pode criar pontos vulneráveis nos sistemas como autenticação inadequada, encriptação inadequada, portas desnecessariamente abertas, controle de acesso insuficiente, entre outras [4].

1.2 Motivação e Justificativa

Com o rápido avanço da tecnologia e o crescente uso de dispositivos IoT, a segurança de dados tornou-se uma preocupação premente para empresas, indústria e usuários. A integridade, confidencialidade e disponibilidade dos dados são fundamentais para garantir a confiança, a utilização adequada e a expansão sustentável desses dispositivos. Contudo, quando a excelência desses três pilares da segurança não são atingidos acontecem ocorrências de vazamentos de dados e invasão através de dispositivos IoT, como foi o caso em que um modelo de câmera da Ring, empresa que pertence à Amazon, foi invadido por usuários maliciosos que utilizaram da vulnerabilidade para fazer ameaças de morte, injúrias raciais e até chantagem [5].

Nesse contexto, este trabalho é norteado pelas seguintes questões de pesquisa (QP):

QP1: Quais são as principais vulnerabilidades de dispositivos IoT encontradas na literatura?

QP2: Quais são as possíveis soluções encontradas na literatura para essas vulnerabilidades?

Dessa forma, este trabalho visa catalogar e categorizar as vulnerabilidades mais comuns presentes nos dispositivos IoT, proporcionando uma visão abrangente das ameaças à segurança da informação percebidas na literatura. A pesquisa também investiga possíveis soluções para as vulnerabilidades encontradas.

1.3 Objetivo geral

O principal objetivo desta pesquisa é elaborar um catálogo sobre as principais vulnerabilidades de dispositivos IoT e medidas de mitigação documentadas na literatura.

Ao identificar e analisar as vulnerabilidades mais comuns nos sistemas IoT, este estudo visa oferecer insights cruciais para o desenvolvimento de melhores práticas na segurança desses dispositivos. Os resultados obtidos contribuirão para fortalecer a segurança, promovendo soluções mais robustas e confiáveis. Assim, este catálogo de vulnerabilidades busca ser uma fonte valiosa para impulsionar a evolução contínua e segura do ecossistema IoT.

1.3.1 Objetivos específicos

- **OE1:** Identificar vulnerabilidades e ataques a dispositivos IoT;
- **OE2:** Descrever e dar exemplos dessas falhas;
- **OE3:** Catalogar as informações trazendo possíveis soluções para as vulnerabilidades encontradas.

1.4 **Estrutura do trabalho**

Este trabalho se encontra dividido em seis capítulos, sendo o primeiro, de introdução, no qual é contextualizado os temas dentro do cenário global atual e apresenta as motivações, justificativas e objetivos do trabalho. O segundo capítulo é composto pelos trabalhos relacionados à pesquisa. No terceiro capítulo é apresentado o referencial teórico da pesquisa. Por conseguinte, há o quarto capítulo, que apresenta a metodologia do estudo e suas fases. No quinto capítulo os resultados serão discutidos. Por fim, no sexto e último capítulo, , bem como apresentadas as conclusões e sugestões de pesquisas futuras.

2 TRABALHOS RELACIONADOS

Uma pesquisa foi realizada no Google Acadêmico utilizando a seguinte string de busca: "IoT vulnerability catalogue"visando encontrar trabalhos relacionados. Os estudos de Rytel [6] e Golendukhina [7] foram encontrados na primeira página, enquanto Kaksonen [8] foi encontrado na segunda página de pesquisa. Um resumo desses trabalhos é apresentado na Figura 1.

Critérios	**Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources (Rytel M.)**	**A Catalog of Consumer IoT Device Characteristics for Data Quality Estimation (Golendukhina V.)**	**Vulnerabilities in IoT devices, backends, applications, and components (Kaksonen R.)**	**Trabalho proposto**
Método de pesquisa	Revisão Bibliográfica	Revisão Bibliográfica	Revisão Bibliográfica	Snowballing
Ano	2020	2024	2023	2024
Objetivo da pesquisa	Contribuir para o aumento da cibersegurança no mundo do IoT através da disponibilização de dados de vulnerabilidades de forma acessível e processável por diferentes tipos de software de segurança.	Desenvolver um catálogo de características de dispositivos de IoT do consumidor para estimativa de qualidade de dados e sintetizar fatores relacionados à qualidade de dados de dispositivos de IoT do consumidor.	Identificar onde e que tipo de vulnerabilidades existem nos sistemas de IoT, investigar onde as vulnerabilidades são mais frequentes e quais são os tipos mais comuns de vulnerabilidades na IoT.	Identificar vulnerabilidades e ataques a dispositivos IoT, descrever e dar exemplos dessas falhas. Além disso, catalogar as informações trazendo possíveis soluções para as vulnerabilidades encontradas.

Figura 1: Trabalhos relacionados

A revisão bibliográfica de Rytel [6] busca identificar e avaliar fontes de informações publicamente disponíveis sobre vulnerabilidades afetando dispositivos IoT, analisar a existência de uma fonte satisfatória que cubra as vulnerabilidades no contexto do IoT, destacar a falta de um serviço único que ofereça dados focados no IoT, propor a criação

de um banco de dados abrangente de vulnerabilidades IoT como um objetivo de longo prazo, avaliar as limitações das bases de dados de vulnerabilidades existentes em lidar com vulnerabilidades IoT e contribuir para o aumento da cibersegurança no mundo do IoT através da disponibilização de dados de vulnerabilidades de forma acessível e processável por diferentes tipos de software de segurança.

Já o estudo de Valentina Golendukhina [7] inclui a identificação e síntese de fatores relacionados à qualidade de dados de dispositivos de IoT do consumidor, o desenvolvimento de um catálogo de características desses dispositivos para estimativa da qualidade de dados, a criação de uma ferramenta de suporte para facilitar a avaliação da qualidade de dados e a realização de um estudo de caso para demonstrar a aplicação do catálogo e avaliar os resultados, com foco nos dados gerados por smartwatches.

Além disso, o estudo de Rauli Kaksonen [8] analisa as vulnerabilidades em sistemas IoT com base em entradas do Common Vulnerabilities and Exposures (CVE) e vulnerabilidades conhecidas exploradas. Os objetivos incluem compreender a distribuição das vulnerabilidades, identificar as categorias de falhas mais importantes, auxiliar pesquisadores e profissionais de segurança a entender melhor a segurança da IoT, identificar onde e que tipo de vulnerabilidades existem nos sistemas de IoT, e investigar as áreas mais vulneráveis e os tipos mais comuns de vulnerabilidades na IoT.

Por fim, este trabalho herda um pouco do que foi abordado no estudo de Rytel [6], Golendukhina [7], Kaksonen [8] e preenche lacunas existentes nesses três estudos:

- Rytel: Não há a catalogação dos dados de vulnerabilidades coletados, além de não trazer as vulnerabilidades mais comuns;
- Golendukhina: Catálogo restrito apenas à qualidade de dados dos dispositivos IoT e não relacionado às suas vulnerabilidades;
- Kaksonen: Apesar de trazer as vulnerabilidades mais comuns em ambientes IoT, não há a preocupação em trazer as possíveis soluções para essas vulnerabilidades.

Além do mais, esse trabalho também se aproxima de dois conhecidos sites no mundo da cibersegurança: MITRE ATT&CK [9] e o OWASP IoT [10]. O MITRE é uma base global de conhecimento de táticas e técnicas adversárias baseadas em observações do mundo real [9]. Enquanto o OWASP IoT é um projeto pensado para ajudar fabricantes, desenvolvedores e consumidores a entender melhor os problemas de segurança associados

à Internet das Coisas e para permitir que usuários em qualquer contexto tomem melhores decisões de segurança ao criar, implantar ou avaliar tecnologias IoT. O projeto procura definir uma estrutura para vários subprojetos de IoT separados nas seguintes categorias - Buscar e Compreender, Validar e Testar e Governança [10]. Contudo, esse estudo se diferencia de ambos pelos presentes motivos:

- MITRE: O MITRE foca em vulnerabilidades e ataques do mundo da cibersegurança de maneira geral, sem enfoque nos ambientes IoT;
- OWASP IoT: Apesar de compartilhar o foco para a internet das coisas, porém não se preocupa em trazer possíveis soluções para os pontos vulneráveis encontrados no projeto.

3 REFERENCIAL TEÓRICO

No cenário tecnológico contemporâneo, a proliferação de Dispositivos da Internet das Coisas (IoT) tem ampliado exponencialmente as possibilidades de conectividade, oferecendo inovações significativas em setores como saúde, automação residencial e indústria. No entanto, essa crescente interconexão também expõe um conjunto complexo de desafios, particularmente no domínio da segurança da informação. Este referencial teórico apresentar os principais conceitos envolvidos neste trabalho, a começar pelas definições sugeridas para IoT, os pilares que sustentam a segurança da informação, as camadas que constituem a rede em ambientes IoT e, por fim, é apresentado o conceito de vulnerabilidade no contexto da segurança.

3.1 Dispositivos IoT

A natureza heterogênea da arquitetura da Internet das Coisas (IoT), envolvendo uma ampla variedade de entidades com diferentes capacidades de recursos, torna um desafio fornecer conexões seguras de ponta a ponta [11].

Dessa forma, um dispositivo IoT é composto por vários componentes, como sensores, atuadores, interfaces de comunicação, sistemas operacionais, software de sistema, aplicativos pré-carregados e serviços leves. A principal função de um dispositivo IoT, ou "coisa inteligente", é coletar informações contextuais por meio de sensores e realizar ações por meio de atuadores. Por exemplo, um termostato inteligente detecta a temperatura e a umidade ambiente, ajustando o ar condicionado de acordo [12].

3.2 Segurança da Informação

A informação é um importante recurso em diversas áreas na vida humana, tornando a segurança de dados uma das principais preocupações na era digital. Nesse contexto, a segurança de qualquer sistema digital é comumente definida usando os três atributos de confidencialidade (C), integridade (I) e disponibilidade (D), também conhecidos como tríade de segurança CID [3].

Portanto, ao entrarmos no domínio da segurança digital, precisamos compreender a maneira pela qual a convergência entre confidencialidade, integridade e disponibilidade

não apenas delimita, mas configura o fundamento essencial capaz de sustentar a resiliência diante dos desafios emergentes no ciberespaço:

- **Confidencialidade**: O sigilo e a confidencialidade das informações transmitidas e armazenadas devem ser rigorosamente preservados. Refere-se a limitar o acesso e divulgação de informações ao nó IoT autorizado e impedir o acesso ou divulgação a pessoas não autorizadas. Por exemplo, uma rede IoT não deve revelar as leituras dos sensores aos seus vizinhos (se estiver configurada para não o fazer) [12].

- **Integridade**: A integridade pode ser definida percebendo-se que a IoT baseia-se na troca de dados entre muitos dispositivos diferentes, por isso é muito importante garantir a precisão dos dados provenientes do remetente certo, bem como garantir que os dados não sejam adulterados durante o processo de transmissão devido a interferência intencional ou não intencional [13]. A integridade também é necessária para fornecer um serviço confiável. O dispositivo deve garantir que os comandos recebidos e as informações coletadas são legítimos [14].

- **Disponibilidade**: A disponibilidade indica o acesso oportuno e confiável de informações ou serviços a entidades autorizadas [15]. A sobrevivência dos serviços em todas as camadas da rede na presença de vulnerabilidades é a medida da disponibilidade na IoT. Devido ao amplo uso global da IoT, a disponibilidade sempre estará presente na lista dos principais requisitos de segurança [16]. Ela garante que os serviços e recursos do sistema estejam instantânea e continuamente disponíveis para os usuários, quando necessário [17].

3.3 Camadas de Rede

Para esta pesquisa, será adotada uma estrutura de sistema distribuído em três camadas. Essa estrutura é capaz de proporcionar uma explicação abrangente dos recursos presentes em ambientes IoT, e é amplamente reconhecida na literatura especializada: [1,13,16,18–23]. Embora alguns artigos sugiram uma estrutura de cinco camadas e outros quatro, a maioria, analisada neste trabalho, adota o modelo de três camadas. Portanto, serão utilizadas as três camadas que aparecem com maior frequência, são elas: a camada de percepção, a camada de transporte ou rede e a camada de aplicação.

Camada de Percepção - Está relacionada aos sensores físicos IoT para apoiar a coleta e processamento de dados em diferentes tecnologias comuns, como identificação por radiofrequência (RFID), rede de sensores sem fio (RSSF), rede de sensores RFID (RSN) e GPS. Esta camada inclui sensores e atuadores para realizar diferentes medições (ou seja, temperatura, aceleração, umidade, etc.) e funcionalidades como consulta de localização [19, 23].

Camada de Transporte(Rede) - A camada de rede da IoT serve a função de roteamento e transmissão de dados para diferentes hubs e dispositivos IoT pela Internet. Nesta camada, plataformas de computação em nuvem, gateways de Internet, dispositivos de comutação e roteamento, etc. operam usando algumas das tecnologias mais recentes, como WiFi, LTE, Bluetooth, 3G, Zigbee, etc. [13].

Camada de Aplicação - A camada de aplicação fornece os serviços solicitados pelos clientes. Por exemplo, a camada de aplicação pode fornecer medições de temperatura e umidade do ar aos clientes que solicitam esses dados. A importância desta camada para a IoT é que ela tem a capacidade de fornecer serviços inteligentes de alta qualidade para atender às necessidades dos clientes [19]. Essa aplicação fornece serviços inteligentes sensíveis ao contexto de maneira abrangente [23].

Um sistema ou serviço IoT confiável depende não apenas da cooperação confiável entre as camadas, mas também do desempenho de todo o sistema e de cada camada do sistema no que diz respeito à segurança, privacidade e outras propriedades relacionadas à confiança. Garantir a confiabilidade de uma camada IoT (por exemplo, camada de rede) não implica que a confiança de todo o sistema possa ser alcançada [23].

3.4 Vulnerabilidade no contexto de Segurança da Informação

Uma vulnerabilidade de segurança pode ser vista como qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a recursos. Elas incluem — mas não se limitam — a itens como softwares mal configurados, aparelhos com sistemas desatualizados e arquivos internos expostos publicamente. Em outras palavras, brechas de segurança são pontos da infraestrutura de TI que tornam mais fácil o acesso não autorizado aos recursos do negócio [24]. Entretanto, também podemos tratar vulnerabilidade como: uma falha ou fraqueza no aplicativo, que pode ser uma falha de design ou um bug de implementação, que permite que um invasor cause danos às partes

interessadas de um aplicativo. As partes interessadas incluem o proprietário do aplicativo, os usuários do aplicativo e outras entidades que dependem do aplicativo [25].

Essas falhas costumam ser publicadas no Open Web Application Security Project, ou OWASP, que é uma organização internacional sem fins lucrativos dedicada a segurança de aplicativos web. Um dos princípios fundamentais do OWASP é que todos os seus materiais estejam disponíveis gratuitamente e facilmente acessíveis em seu site, tornando possível para qualquer pessoa melhorar a segurança de seus próprios aplicativos web [26].

Contudo, o OWASP tem um projeto que foi desenvolvido em 2014 apenas para a Internet das Coisas. O OWASP IoT Top 10 representa as dez principais coisas a serem evitadas ao construir, implantar e gerenciar sistemas IoT. Em vez de ter listas separadas para riscos versus ameaças versus vulnerabilidades, ou para desenvolvedores versus empresas versus consumidores, a equipe do projeto optou por ter uma lista única e unificada que captura os principais itens a serem evitados ao lidar com segurança de IoT [10].

4 METODOLOGIA

Este estudo buscou investigar e analisar as vulnerabilidades em dispositivos IoT, bem como as soluções propostas na literatura científica. O processo metodológico foi delineado em etapas que visam garantir uma abordagem abrangente na seleção e análise dos artigos relevantes. Foram utilizadas três etapas:

- **Pesquisa inicial:** Identificação dos primeiros artigos com a utilização do Google Acadêmico;
- **Snowballing:** Identificação e coleta de novos estudos que abordam a segurança de dispositivos IoT, a partir dos estudos iniciais;
- **Elaboração de catálogo:** Utilização de critérios para avaliação de falhas de segurança em dispositivos IoT.

Inicialmente, conduziu-se uma pesquisa no Google Acadêmico, empregando uma variedade de strings de busca em inglês e português relacionadas às vulnerabilidades em dispositivos IoT. As strings incluíam termos como 'iot vulnerabilities systematic review', 'vulnerabilities in iot' e 'what makes iot so insecure?'. A busca foi realizada utilizando diferentes combinações de termos, com o objetivo de abranger o máximo de conteúdo relevante disponível na literatura. Foi conseguido uma média de 70 mil resultados durante as buscas, percorrendo duas a três páginas por resultado.

A percepção obtida durante a pesquisa revelou que, embora muitos artigos abordassem a segurança em IoT, a maioria estava mais voltada para os protocolos existentes nas redes do que para as vulnerabilidades e ataques em si. Essa observação ressalta a necessidade de um maior enfoque em estudos que abordem diretamente as vulnerabilidades e os ataques enfrentados por dispositivos IoT, a fim de fortalecer a segurança nesse campo em rápida evolução.

Após essa pesquisa inicial, foram selecionados 12 artigos com base em critérios de relevância e qualidade:

- Relação do artigo com o tema de estudo;
- Trabalhos escritos apenas em inglês e português;

- Estudos com data de publicação entre 2013 e 2023;
- Artigos com menos de quatro páginas não foram aceitos.

Foram considerados apenas estudos que abordavam vulnerabilidades em dispositivos IoT, soluções propostas para mitigar essas vulnerabilidades e estudos relacionados. Ver Tabela 1.

Tabela 1: Artigos iniciais

ID	**Título**	**Autor**	**Snowballing**
1	IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices	MENEGHELLO, F. et al. (2019) [1]	7 Artigos
2	Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations	NESHENKO, N. et al. (2019) [4]	11 Artigos
3	Securing the Internet of Things (IoT): A Security Taxonomy for IoT	RIZVI, S. et al. (2018) [18]	3 Artigos
4	Security threats in IoT	DOROBANTU, O. G.; HALUNGA, S. (2020) [27]	1 Artigo
5	Secure IoT: An Improbable Reality	MANNILTHODI, N.; KANNIMOOLA, J. M. (2017) [28]	2 Artigos
6	Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects	SRIVASTAVA, A. et al. (2020) [16]	0 Artigos
7	Root Causes of Insecure Internet of Things and Holistically Addressing Them	WHITE, C. A. (2020) [3]	3 Artigos
8	IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids	ANAND, P. et al. (2020) [20]	0 Artigos
9	Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review	LIAO, B. et al. (2020) [29]	0 Artigos
10	Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review	MISHRA, N.; PANDYA, S. (2021) [30]	0 Artigos
11	A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain	POURRAHMANI, H. et al. (2023) [15]	0 Artigos
12	Segurança da informação em IOT	FUKUDA, L. M. (2019) [2]	0 Artigos
Fonte: O Autor.			

Além disso, para elaboração do catálogo, este estudo utilizou a técnica snowballing para trás [31], que se refere a utilização das referências bibliográficas de um artigo para identificar novos trabalhos que possam agregar ao estudo. Esse procedimento foi feito

de forma progressiva, a partir dos estudos encontrados inicialmente, a fim de trazer uma maior base teórica ao estudo.

Uma vez identificados os 12 estudos relevantes, mais os 27 estudos adquiridos através do snowballing procedeu-se à catalogação das vulnerabilidades identificadas em cada artigo. Foi elaborada uma planilha[1], na qual foram registradas informações específicas sobre cada vulnerabilidade, incluindo descrição, contexto de aplicação, soluções propostas e as referências para os artigos nas quais foram encontaradas. Além disso, para cada um desses estudos foi realizado um snowballing para trás, agregando mais 27 estudos além dos 12 iniciais. Os 27 estudos obtidos por meio do snowballing são listados na Tabela 2.

Tabela 2: Snowballing

ID	Título	Autor	Snowballing
1	Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things	MENEGHELLO, HOSSAIN, M. M.; FOTOUHI, M.; HASAN, R. (2015) [12]	[1]
2	Collaborative security for the internet of things	SAIED, Y. B. (2013) [11]	[1]
3	A Survey on the Internet of Things Security	ZHAO, K.; GE, L. (2013) [21]	[1]
4	A survey on trust management for Internet of Things	YAN, Z.; ZHANG, P.; VASILAKOS, A. V. (2014) [23]	[1]
5	Evaluating Critical Security Issues of the IoT World: Present and Future Challenges	FRUSTACI, M. et al. (2018) [19]	[1]
6	The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved	ZHOU, W. et al. (2019) [32]	[1]
7	A Comprehensive Study of Security of Internet-of-Things	MOSENIA, A.; JHA, N. K. (2017) [14]	[1, 4]
8	HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities	STANISLAV, M.; BEARDSLEY, T. (2015) [33]	[4]
9	Botnets and Internet of Things Security	BERTINO, E.; ISLAM, N. (2017) [34]	[4]
10	Breaking Down Mirai: An IoT DDoS Botnet Analysis	HERZBERG, D. B. B.; ZIFMAN., I. (2016) [35]	[4]
11	Security, privacy and trust in Internet of Things: The road ahead	SICARI, S. et al. (2015) [22]	[4]
12	Understanding the Mirai Botnet	ANTONAKAKIS, M. et al. (2017) [36]	[4]
13	Sybil attack in IoT: Modelling and defenses	RAJAN, A.; JITHISH, J.; SANKARAN, S. (2017) [37]	[4]
14	Routing Attacks and Countermeasures in the RPL-Based Internet of Things	WALLGREN, L.; RAZA, S.; VOIGT, T. (2013) [38]	[4]
15	You've Got Vulnerability: Exploring Effective Vulnerability Notifications	LI, F. et al. (2016) [39]	[4]
16	Inferring, Characterizing, and Investigating Internet-Scale Malicious IoT Device Activities: A Network Telescope Perspective	TORABI, S. et al. (2018) [40]	[4]
17	Survey of Attack Projection, Prediction, and Forecasting in Cyber Security	HUSÁK, M. et al. (2019) [41]	[4]
18	On the inference and prediction of DDoS campaigns	FACHKHA, C.; BOU-HARB, E.; DEBBABI, M. (2015) [42]	[4]
19	OWASP Internet of Things Project	OWASP (2018) [10]	[18]
20	Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures	MAHMOUD, R. et al. (2015) [13]	[18]
21	A Survey on Security and Privacy Issues in Internet-of-Things	YANG, Y. et al. (2017) [43]	[18]
22	Attacks and Defenses in Short-Range Wireless Technologies for IoT	LOUNIS, K.; ZULKERNINE, M. (2020) [17]	[27]
23	A Survey on Detection of Sinkhole Attack in Wireless Sensor Network	KIBIRIGE, G. W.; SANGA, C. (2015) [44]	[28]
24	Uninvited Connections A Study of Vulnerable Devices on the Internet of Things (IoT)	PATTON, M. et al. (2014) [45]	[28]
25	Foundational Cybersecurity Activities for IoT Device Manufacturers	FAGAN, M. et al. (2020) [46]	[3]
26	2020 Unit 42 IoT Threat Report	Unit 42 (2020) [47]	[3]
27	Security Issues in the Internet of Things (IoT): A Comprehensive Study	RAZZAQ, M. A. et al. (2017) [48]	[3]

Fonte: O Autor.

[1] A planilha pode ser acessada aqui: https://docs.google.com/spreadsheets/d/1cTYLaTgoZArXOi9hiCfMA4gRt0gSMxRTiPF7AzEREA/edit?usp=sharing

Cada vulnerabilidade catalogada foi pontuada com base em sua frequência de aparição nos artigos selecionados. A pontuação proporciona uma visão quantitativa das vulnerabilidades mais prevalentes na literatura analisada. Esta análise permitiu uma compreensão aprofundada das vulnerabilidades em dispositivos IoT, fornecendo insights sobre as ameaças mais comuns e as estratégias de mitigação propostas na literatura científica.

5 RESULTADOS

Na era da conectividade ubíqua, os dispositivos IoT (Internet das Coisas) desempenham um papel vital em nossas vidas cotidianas. No entanto, essa interconexão também introduz um conjunto significativo de desafios, destacados pelas inúmeras vulnerabilidades identificadas na literatura especializada.

A partir dos estudos selecionados, foram identificadas as vulnerabilidade descritas na Figura 2. Esta lista de vulnerabilidades destaca os principais pontos de fragilidade encontrados em dispositivos IoT, fornecendo uma visão abrangente dos riscos enfrentados por essa tecnologia emergente.

Nos estudos coletados, uma tendência notável emerge, evidenciando a predominância de certas vulnerabilidades no cenário da segurança cibernética. Em particular, cinco vulnerabilidades se destacaram por serem as mais comuns, são elas: DDoS, Botnets, Inadequate authentication, Improper encryption e Jamming and Radio Interference, como pode ser visto na Figura 2.

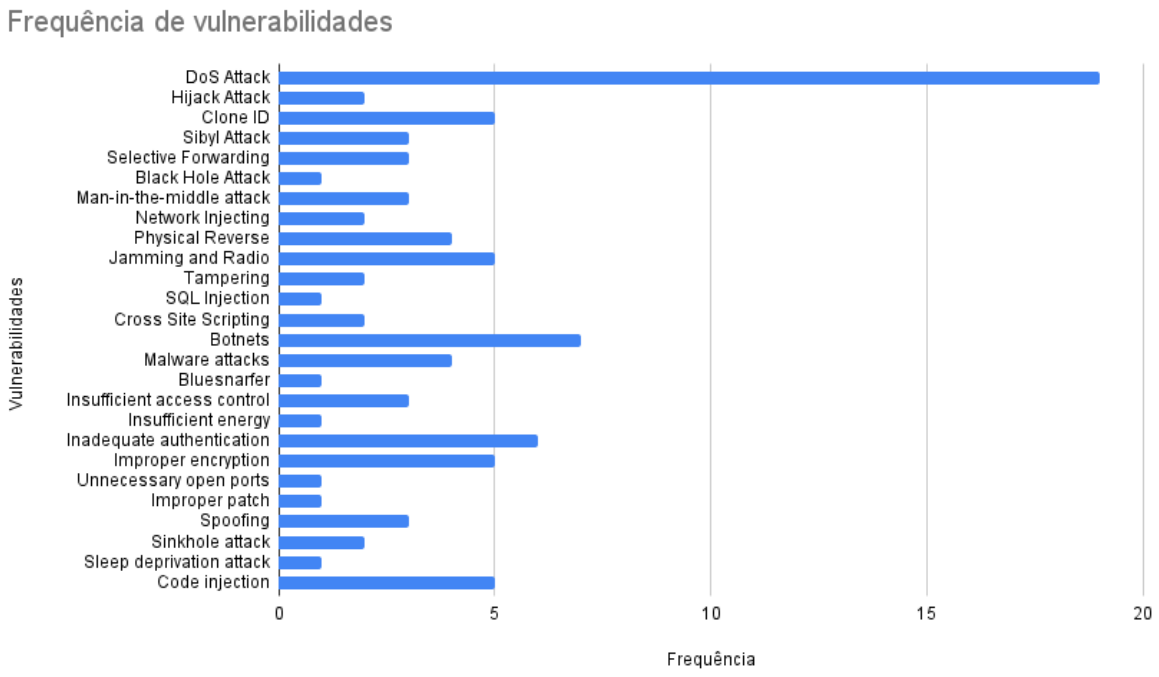

Figura 2: Frequência das vulnerabilidades encontradas nos artigos coletados

Entre essas, o ataque de negação de serviço (DDoS) sobressai-se como a vulnerabilidade mais recorrente. Esse tipo de ataque visa sobrecarregar os recursos de um

sistema alvo, tornando-o inacessível para usuários legítimos. Sua prevalência é uma preocupação significativa, dada a capacidade de interromper serviços vitais e causar prejuízos substanciais.

Além disso, a presença proeminente de Botnets indica a complexidade e a escala dos ataques coordenados que podem ser lançados contra infraestruturas digitais. Botnets são redes de dispositivos comprometidos controlados remotamente por um invasor, permitindo a execução de ações maliciosas em massa.

A questão da autenticação inadequada e da criptografia imprópria também merece atenção especial. Essas vulnerabilidades ressaltam a importância crítica de proteger o acesso a sistemas e dados confidenciais. Falhas nessas áreas podem resultar em violações de segurança graves, comprometendo a confidencialidade e a integridade das informações.

Além disso, ataques como Jamming and Radio Interference ilustram a diversidade de vetores de ataque, aproveitando falhas em comunicações sem fio para interferir ou interromper operações essenciais. Esses tipos de ataques destacam a necessidade de abordagens robustas de segurança que considerem uma ampla gama de ameaças potenciais.

Por fim, as vulnerabilidades relacionadas a códigos, como Code injection, e a manipulação de dados, como Malware attacks, ressaltam a importância de garantir a integridade e a segurança dos sistemas contra explorações de vulnerabilidades em software e ataques de malware.

Contudo, na literatura, determinadas vulnerabilidades emergem como tendo uma quantidade significativa de soluções propostas para mitigar seus riscos. Entre essas vulnerabilidades, destacam-se: DDoS, Clone ID, Inadequate authentication, Improper encryption, Malware attacks, Man-in-the-middle attack, Botnets, Insufficient access control, Sibyl Attack e Selective Forwarding, como mostra a Figura 4.

A considerável quantidade de soluções abordando o ataque de negação de serviço (DDoS) reflete a sua relevância e a urgência de contra-medidas eficazes. Estratégias para detectar, mitigar e responder a ataques DDoS são amplamente discutidas, dada a sua capacidade de interromper serviços online e causar danos substanciais.

Além disso, a presença de soluções para Clone ID e Inadequate authentication sublinha a importância da autenticação robusta e da proteção contra roubo de identidade e acesso não autorizado. Essas medidas são essenciais para garantir a integridade e a confidencialidade dos sistemas e dados.

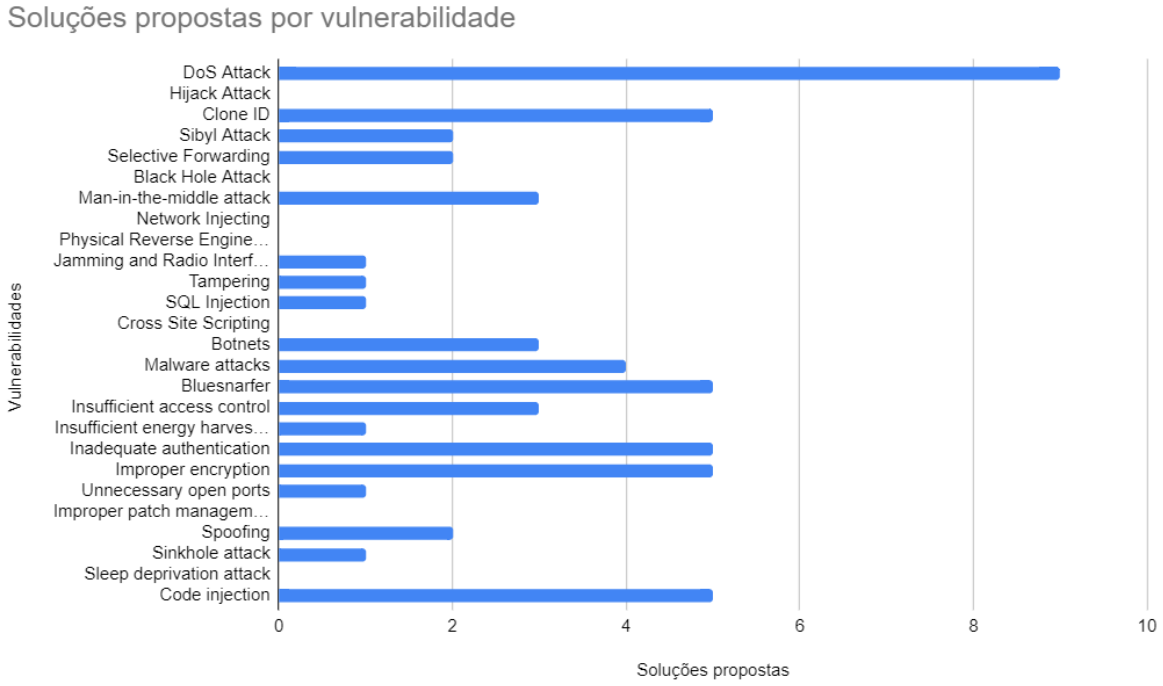

Figura 3: Soluções propostas para cada vulnerabilidade encontrada na literatura

Em resumo, a análise das soluções propostas para essas vulnerabilidades destaca a importância da pesquisa contínua e do desenvolvimento de estratégias eficazes de segurança cibernética para proteger ativos digitais contra uma variedade de ameaças cada vez mais sofisticadas.

As vulnerabilidades podem ser classificadas segundo várias perspectivas, sendo assim, elas podem ser categorizadas seguindo os seguintes critérios:

- Vulnerabilidades relacionadas a segurança física;
- Vulnerabilidades relacionadas a Autenticação e Autorização;
- Vulnerabilidades por camada de rede;
- Tríade CID;

5.1 **Vulnerabilidades relacionadas a segurança física**

Referem-se a falhas ou fragilidades em um sistema, infraestrutura ou dispositivo que podem ser exploradas por um invasor para comprometer a integridade, confidencialidade ou disponibilidade dos recursos físicos. Essas vulnerabilidades, listadas na Figura 4,

podem ocorrer em uma variedade de contextos, incluindo instalações físicas, equipamentos de hardware e dispositivos eletrônicos.

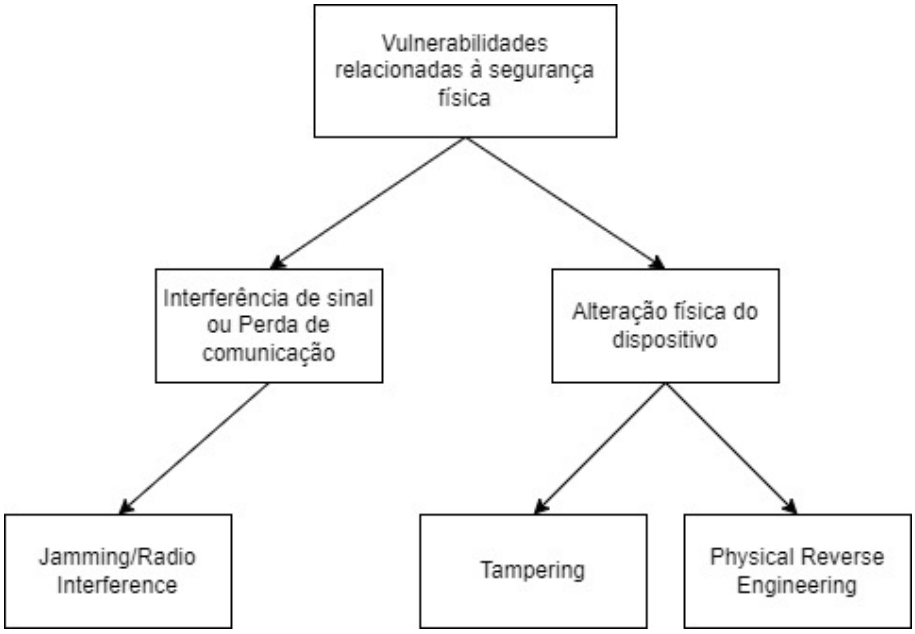

Figura 4: Segurança de hardware

5.2 **Vulnerabilidades relacionadas a Autenticação e Autorização**

Referem-se a falhas ou lacunas em sistemas de segurança que lidam com a identificação e verificação de usuários, bem como a concessão de permissões de acesso a recursos ou funcionalidades específicas. Essas vulnerabilidades podem permitir que indivíduos não autorizados obtenham acesso indevido a sistemas, dados ou recursos protegidos (Tabela 3).

5.3 **Vulnerabilidades por camada de rede**

Na interconexão cada vez mais intrincada de dispositivos e sistemas, a segurança de redes torna-se um pilar crítico para salvaguardar a integridade, confidencialidade e disponibilidade dos dados transmitidos. Este capítulo, explora a complexidade das falhas de segurança que podem surgir em diferentes estratos da arquitetura de rede.

Ao mergulharmos nas distintas camadas que compõem a infraestrutura de comunicação, percebemos os pontos críticos (como mostrados na Tabela 4) onde vulnerabilidades podem ser exploradas. A análise dessas vulnerabilidades proporciona uma compre-

Vulnerabilidade	Autenticação	Autorização
Clone ID	Sim	Não
Man-in-the-middle attack	Sim	Não
SQL Injection	Sim	Sim
Cross Site Scripting	Sim	Sim
Bluesnarfer	Sim	Sim
Spoofing	Sim	Não
Insufficient access control	Sim	Sim
Botnets	Sim	Sim
Insufficient energy harvesting	Não	Sim
Inadequate authentication	Sim	Sim
Improper encryption	Não	Sim
Sinkhole attack	Não	Sim
Code injection	Não	Sim

Tabela 3: Vulnerabilidades relacionadas à autenticação e autorização

ensão aprofundada dos desafios enfrentados na proteção das redes contra ameaças cada vez mais sofisticadas.

5.4 **Catálogo de vulnerabilidades**

O catálogo de segurança proposto é estruturado de forma a abordar diferentes falhas de segurança encontradas em sistemas IoT, fornecendo uma visão detalhada de cada uma delas. Cada entrada no catálogo é composta pelos seguintes elementos:

- Nome da Falha: Identifica o tipo específico de vulnerabilidade ou falha de segurança em sistemas IoT.
- Imagem Explicativa: Apresenta uma representação visual da falha de segurança para facilitar a compreensão do leitor.
- Descrição: Oferece uma explicação detalhada da falha de segurança, incluindo como ela ocorre, quais são seus efeitos e quais são os possíveis vetores de ataque.
- Exemplo: Apresenta um caso de uso ou cenário onde a falha de segurança poderia ser explorada por um atacante, ilustrando sua relevância e impacto potencial.
- Tríade CID: Analisa a falha de segurança sob a perspectiva da tríade de segurança CID, destacando como ela afeta os atributos de Confidencialidade, Integridade e Disponibilidade do sistema.

- Possíveis Soluções: Sugere abordagens ou contramedidas para mitigar ou prevenir a falha de segurança, visando fortalecer a segurança do sistema IoT contra possíveis ataques.

Além disso, o catálogo é composto por um total de seis padrões de segurança propostos com base nas vulnerabilidades mais citadas.

5.4.1 Distributed Denial of Service (DDoS)

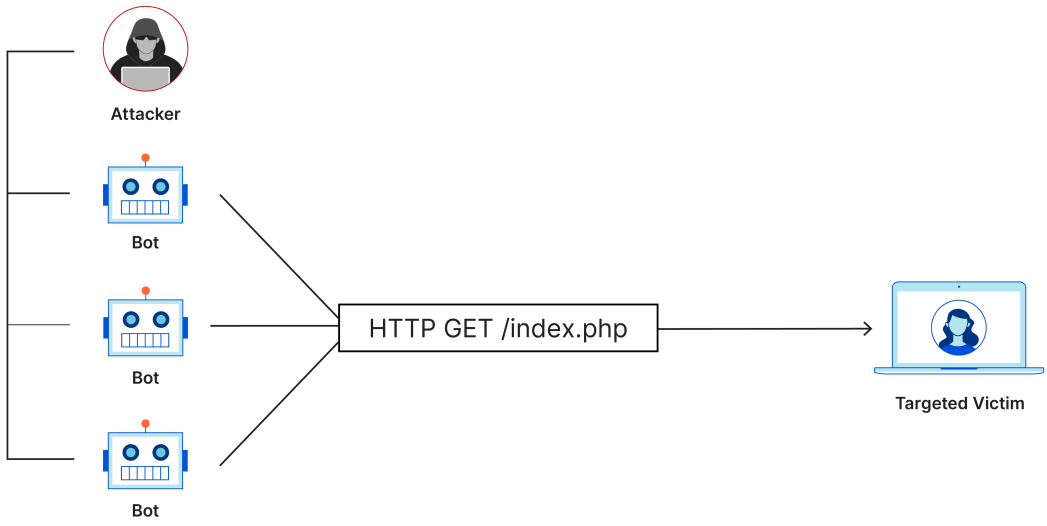

Figura 5: Ataque de negação de serviço. **Fonte**: www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/

Descrição: Um ataque DoS ocorre quando um invasor usa seus próprios ativos para solicitar conexões a um servidor que permite serviços a diferentes usuários, inevitavelmente congestionando e paralisando o servidor que está habilitando os serviços. Um ataque DDoS ocorre quando um invasor (botmaster) utiliza bots (computadores controlados pelo invasor que podem não ser conhecidos pelo proprietário do computador) para solicitar um servidor que habilite serviços para diferentes usuários. Isso cria uma sobrecarga de solicitações que inevitavelmente derrubam o servidor. Na IoT, a ameaça de um ataque DDoS é contínua.

Exemplo: O maior ataque de DDoS até hoje ocorreu em setembro de 2017. O ataque visou os serviços do Google e atingiu um tamanho de 2,54 Tbps. O Google Cloud divulgou o ataque em outubro de 2020. Os invasores enviaram pacotes falsificados para

180.000 servidores web que, por sua vez, enviaram respostas ao Google. Esse ataque não foi um incidente isolado: os invasores haviam direcionado vários ataques de DDoS à infraestrutura do Google nos seis meses que o antecederam.

Tríade CID: Disponibilidade.

Possível solução: Modelos de detecção e prevenção de intrusões para mitigar esses tipos de ataque [30].

5.4.2 Botnets

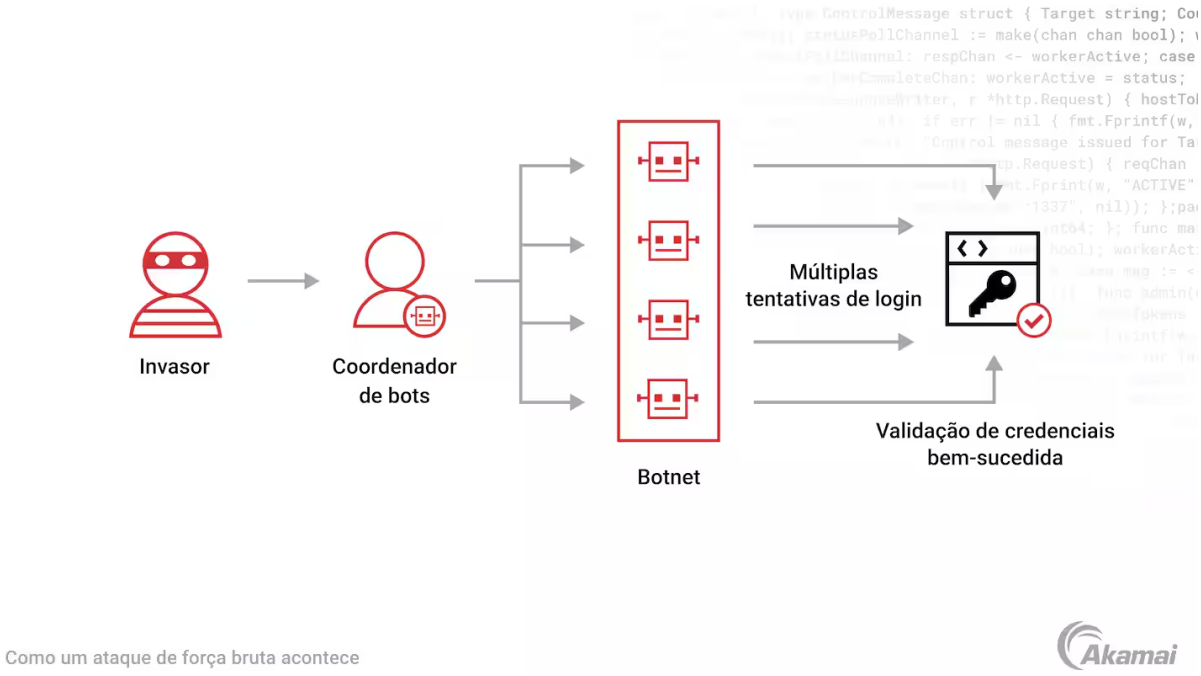

Figura 6: Botnets. **Fonte**: https://www.akamai.com/pt/glossary/what-is-a-botnet

Descrição:Botnet é uma rede de nós controlados remotamente por um adversário para realizar ataques DDoS, distribuir malware, roubar dados privados e enviar spam ou e-mails de phishing [28].

Exemplo: Rustock foi um botnet que se espalhou como um cavalo de Tróia, infectando documentos baixados da Internet ou recebidos como arquivo anexo a um e-mail. As máquinas infectadas enviavam mais de 20.000 mensagens de spam por hora quando ativo (2006). Ele infectou entre 150.000 e 2.400.000 máquinas.

Tríade CID: Disponibilidade.

Possível solução: Segmentação de rede e monitoramento de padrões de tráfego incomuns [28].

5.4.3 Inadequate authentication

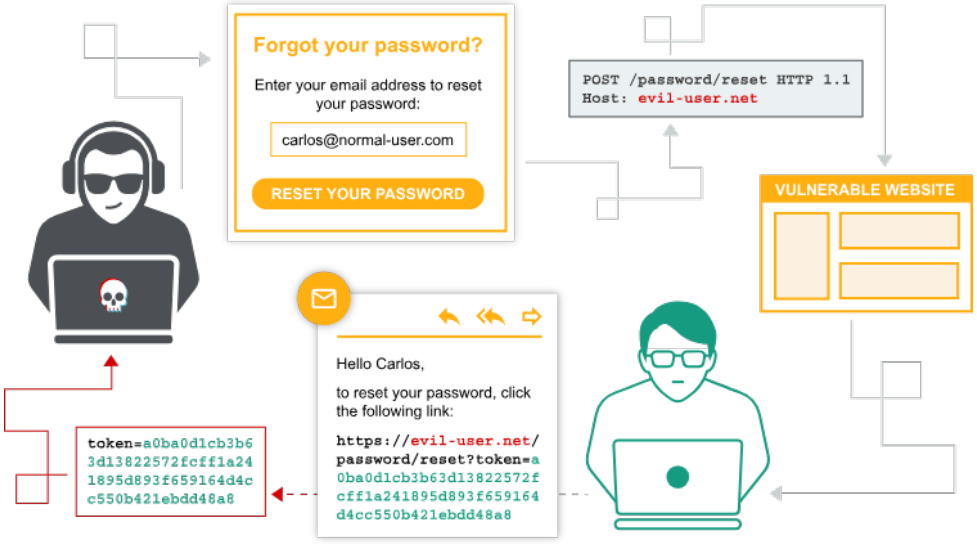

Figura 7: Autenticação inadequada. **Fonte**: https://portswigger.net/web-security/authentication

Descrição: Para este fim, um invasor pode explorar abordagens de autenticação ineficazes para anexar nós maliciosos falsificados ou violar a integridade dos dados, invadindo assim os dispositivos IoT e as comunicações de rede [4].

Exemplo: Em 24,6% dos ataques contra IoT em 2018, '123456' foi a senha utilizada [3].

Tríade CID:Confidencialidade e Integridade.

Possível solução: Para evitar este ataque, a criptografia de dados deve ser aplicada entre o gateway e os sensores ou pode ser aplicada a autenticação do usuário para a detecção de partes não autorizadas [48].

5.4.4 Improper encryption

Descrição: Devido à baixa capacidade computacional, os dispositivos IoT podem evitar a criptografia de transporte ou usar criptografia fraca. Portanto, a comunicação torna-se fácil de descobrir e rastreável pelos agentes maliciosos [12].

Exemplo: Os aplicativos móveis podem suportar vários protocolos ou algoritmos de criptografia para estabelecer conexões seguras. Se a criptografia fraca for permitida como opção alternativa, os invasores poderão explorar essa fraqueza e forçar o aplicativo

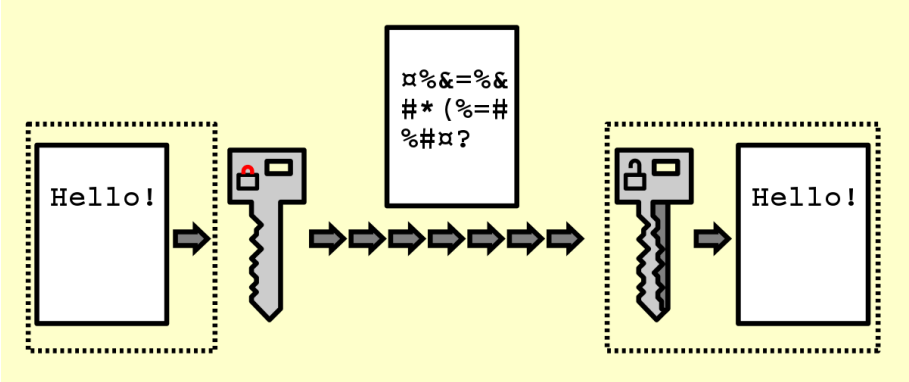

Figura 8: Improper encryption. **Fonte**: https://en.wikipedia.org/wiki/Encryption

a usar criptografia fraca. Como resultado, eles podem descriptografar os dados interceptados com mais facilidade e lançar ataques subsequentes.

Tríade CID: Confidencialidade e Integridade.

Possível solução: Utilizar um esquema de criptografia leve para casas inteligentes baseado em criptografia baseada em identidade (IBE), na qual as chaves públicas são apenas cadeias de identidade sem a necessidade de um certificado digital [43].

5.4.5 Jamming and Radio Interference

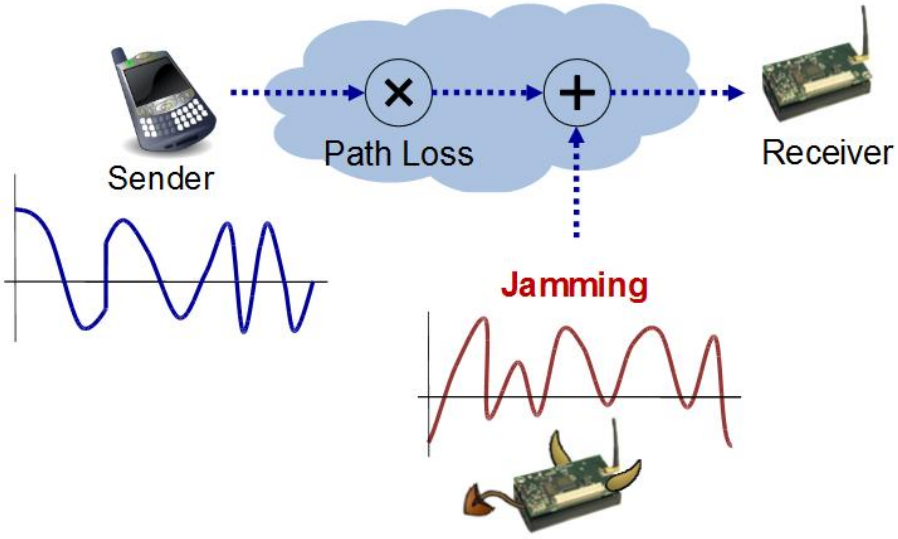

Figura 9: Jamming. **Fonte**: https://mews.sv.cmu.edu/research/jamming/

Descrição: Jamming ocorre quando um invasor usa um dispositivo para interromper a conectividade de um dispositivo IoT. O invasor deve estar nas proximidades do

dispositivo vulnerável. Interferência de rádio é o bloqueio não intencional da conectividade de um dispositivo. Isso também pode ser devido ao ambiente ou à confiabilidade do próprio dispositivo.

Exemplo: Ao tentar se comunicar com outro dispositivo IoT, o sinal emitido é interrompido através de um sinal contrário que anula o inicial. Isso pode acontecer quando dispositivos se comunicam através do wifi, que emite ondas que podem ser percebidas como um padrão e assim ter seu sinal atrasado (gerando lentidão) ou até completamente cortado.

Tríade CID: Disponibilidade.

Possível solução: Ligue o firewall, aplique filtragem de pacotes, anti-bloqueio, bloqueio ativo e programas antivírus atualizados para proteger a rede contra tais ataques [48].

Camada	**Vulnerabilidades**
Camada de Percepção	• Jamming and Radio Interference • Tampering • Physical Reverse Engineering
Camada de Transporte (Rede)	• Botnets • DDoS • Selective Forwarding • Man-in-the-middle attack • Network Injecting • Black Hole Attack • Sleep deprivation attack • Hijack Attack • Clone ID • Sibyl Attack • Malware attacks • Insufficient access control • Improper encryption • Unnecessary open ports • Sinkhole attack • Spoofing
Camada de Aplicação	• SQL Injection • Cross Site Scripting (XSS) • Bluesnarfer • Inadequate authentication • Code injection • Insufficient energy harvesting • Improper patch management capabilities

Tabela 4: Vulnerabilidades por Camada de Rede

6 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho destaca a importância da análise minuciosa das vulnerabilidades em dispositivos de Internet das Coisas (IoT) para fortalecer a segurança da informação nesse ambiente tecnológico em rápida evolução. Ao identificar e catalogar 26 vulnerabilidades, como DDoS, Hijack Attack, Man-in-the-middle attack, entre outras, o estudo proporciona uma visão abrangente das ameaças enfrentadas pelos dispositivos IoT. A pontuação das vulnerabilidades com base em sua frequência de aparição nos artigos selecionados oferece uma perspectiva quantitativa das principais fragilidades presentes na literatura analisada.

Ademais, a análise das soluções propostas para mitigar essas vulnerabilidades visa não apenas compreender os desafios de segurança, mas também fornecer insights para o desenvolvimento de melhores práticas e estratégias de proteção. Ao destacar as vulnerabilidades mais prevalentes e as estratégias de mitigação propostas, este estudo busca contribuir significativamente para o fortalecimento da segurança dos dispositivos IoT e para a promoção de um ambiente mais confiável e seguro para a utilização dessas tecnologias.

Fica claro, dessa forma, que a catalogação detalhada das vulnerabilidades, juntamente com a análise das soluções de segurança, representa um passo importante na compreensão e na abordagem proativa das ameaças cibernéticas em dispositivos IoT. Esses resultados não apenas enriquecem o conhecimento existente sobre as vulnerabilidades nesse campo, mas também fornecem subsídios essenciais para a implementação de medidas eficazes de proteção e para o desenvolvimento contínuo de estratégias de segurança mais robustas e eficientes no contexto da Internet das Coisas.

Para os trabalhos futuros, sugere-se a validação do catálogo por profissionais especializados na área, a fim de garantir sua precisão e relevância prática. Além disso, é recomendável realizar uma análise comparativa entre o estado da prática e o estado da arte, visando identificar lacunas e oportunidades de melhoria. Uma revisão sistemática da literatura também é sugerida como um trabalho futuro, com o intuito de fornecer uma visão abrangente e atualizada sobre o tema, destacando os avanços mais recentes e as áreas de pesquisa promissoras a serem exploradas.

REFERÊNCIAS

[1] MENEGHELLO, F. et al. Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, v. 6, n. 5, p. 8182–8201, 2019.

[2] FUKUDA, L. M. Segurança da informação em iot. Universidade Tecnológica Federal do Paraná, 2019.

[3] WHITE, C. A. Root causes of insecure internet of things and holistically addressing them. In: IEEE. *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. [S.l.], 2020. p. 1066–1074.

[4] NESHENKO, N. et al. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 3, p. 2702–2733, 2019.

[5] PAUL, K. Dozens sue amazon's ring after camera hack leads to threats and racial slurs. *The Guardian. https://www. theguardian. com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats*, 2020.

[6] RYTEL, M.; FELKNER, A.; JANISZEWSKI, M. Towards a safer internet of things—a survey of iot vulnerability data sources. *Sensors*, MDPI, v. 20, n. 21, p. 5969, 2020.

[7] GOLENDUKHINA, V. et al. A catalog of consumer iot device characteristics for data quality estimation. *ACM Journal of Data and Information Quality*, ACM New York, NY, 2024.

[8] KAKSONEN, R.; HALUNEN, K.; RÖNING, J. Vulnerabilities in iot devices, backends, applications, and components. In: SCITEPRESS. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*. [S.l.], 2023.

[9] MITRE. *ATTCK Matrix for Enterprise*. `https://attack.mitre.org`. Acessado em: (23/03/2024).

[10] OWASP. *OWASP Internet of Things Project*. 2018. `https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project`. Acessado em: (08/03/2024).

[11] SAIED, Y. B. *Collaborative security for the internet of things*. Tese (Theses) — Institut National des Télécommunications, jun. 2013. Available at: <https://theses.hal.science/tel-00879790>.

[12] HOSSAIN, M. M.; FOTOUHI, M.; HASAN, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In: *2015 IEEE World Congress on Services*. [S.l.: s.n.], 2015. p. 21–28.

[13] MAHMOUD, R. et al. Internet of things (iot) security: Current status, challenges and prospective measures. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. [S.l.: s.n.], 2015. p. 336–341.

[14] MOSENIA, A.; JHA, N. K. A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, v. 5, n. 4, p. 586–602, 2017.

[15] POURRAHMANI, H. et al. A review of the security vulnerabilities and countermeasures in the internet of things solutions: A bright future for the blockchain. *Internet of Things*, v. 23, p. 100888, 2023. ISSN 2542-6605. Available at: <https://www.sciencedirect.com/science/article/pii/S2542660523002111>.

[16] SRIVASTAVA, A. et al. Future iot-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, v. 33, n. 12, p. e4443, 2020. E4443 IJCS-19-0930.R3. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4443>.

[17] LOUNIS, K.; ZULKERNINE, M. Attacks and defenses in short-range wireless technologies for iot. *IEEE Access*, v. 8, p. 88892–88932, 2020.

[18] RIZVI, S. et al. Securing the internet of things (iot): A security taxonomy for iot. In: IEEE. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. [S.l.], 2018. p. 163–168.

[19] FRUSTACI, M. et al. Evaluating critical security issues of the iot world: Present and future challenges. *IEEE Internet of Things Journal*, v. 5, n. 4, p. 2483–2495, 2018.

[20] ANAND, P. et al. Iovt: Internet of vulnerable things? threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications

towards smart grids. *Energies*, v. 13, n. 18, 2020. ISSN 1996-1073. Available at: <https://www.mdpi.com/1996-1073/13/18/4813>.

[21] ZHAO, K.; GE, L. A survey on the internet of things security. In: *2013 Ninth International Conference on Computational Intelligence and Security*. [S.l.: s.n.], 2013. p. 663–667.

[22] SICARI, S. et al. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, v. 76, p. 146–164, 2015. ISSN 1389-1286. Available at: <https://www.sciencedirect.com/science/article/pii/S1389128614003971>.

[23] YAN, Z.; ZHANG, P.; VASILAKOS, A. V. A survey on trust management for internet of things. *Journal of Network and Computer Applications*, v. 42, p. 120–134, 2014. ISSN 1084-8045. Available at: <https://www.sciencedirect.com/science/article/pii/S1084804514000575>.

[24] MARCONDES, J. S. *Vulnerabilidade de Segurança: O que é, Classificação, Exemplos*. 2022. `https://gestaodesegurancaprivada.com.br/vulnerabilidade-de-seguranca-o-que-e-classificacao-exemplos/#:~:text=Uma%20vulnerabilidade%20de%20segurana%20pode,de%20segurana%20despreparadas%20e%20etc.` Acessado em: (07/03/2024).

[25] OWASP. *Vulnerabilities*. `https://owasp.org/www-community/vulnerabilities/`. Acessado em: (08/03/2024).

[26] CLOUDFLARE. *O que é OWASP? O que é o OWASP Top 10?* `https://www.cloudflare.com/pt-br/learning/security/threats/owasp-top-10/`. Acessado em: (08/03/2024).

[27] DOROBANTU, O. G.; HALUNGA, S. Security threats in iot. In: IEEE. *2020 International Symposium on Electronics and Telecommunications (ISETC)*. [S.l.], 2020. p. 1–4.

[28] MANNILTHODI, N.; KANNIMOOLA, J. M. Secure iot: An improbable reality. In: *IoTBDS*. [S.l.: s.n.], 2017. p. 338–343.

[29] LIAO, B. et al. Security analysis of iot devices by using mobile computing: a systematic literature review. *IEEE Access*, IEEE, v. 8, p. 120331–120350, 2020.

[30] MISHRA, N.; PANDYA, S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, v. 9, p. 59353–59377, 2021.

[31] JALALI, S.; WOHLIN, C. Systematic literature studies: database searches vs. backward snowballing. In: *Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement*. [S.l.: s.n.], 2012. p. 29–38.

[32] ZHOU, W. et al. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, v. 6, n. 2, p. 1606–1616, 2019.

[33] STANISLAV, M.; BEARDSLEY, T. Hacking iot: A case study on baby monitor exposures and vulnerabilities. *Rapid7 Report*, 2015.

[34] BERTINO, E.; ISLAM, N. Botnets and internet of things security. *Computer*, v. 50, n. 2, p. 76–79, 2017.

[35] HERZBERG, D. B. B.; ZIFMAN., I. *Breaking Down Mirai: An IoT DDoS Botnet Analysis*. `https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/?redirect=Incapsula`. Acessado em: (09/03/2024).

[36] ANTONAKAKIS, M. et al. Understanding the mirai botnet. In: *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017. p. 1093–1110. ISBN 978-1-931971-40-9. Available at: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>.

[37] RAJAN, A.; JITHISH, J.; SANKARAN, S. Sybil attack in iot: Modelling and defenses. In: *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. [S.l.: s.n.], 2017. p. 2323–2327.

[38] WALLGREN, L.; RAZA, S.; VOIGT, T. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, v. 9, n. 8, p. 794326, 2013. Available at: <https://doi.org/10.1155/2013/794326>.

[39] LI, F. et al. You've got vulnerability: Exploring effective vulnerability notifications. In: *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, 2016. p. 1033–1050. ISBN 978-1-931971-32-4. Available at: <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/li>.

[40] TORABI, S. et al. Inferring, characterizing, and investigating internet-scale malicious iot device activities: A network telescope perspective. In: *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. [S.l.: s.n.], 2018. p. 562–573.

[41] HUSáK, M. et al. Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys Tutorials*, v. 21, n. 1, p. 640–660, 2019.

[42] FACHKHA, C.; BOU-HARB, E.; DEBBABI, M. On the inference and prediction of ddos campaigns. *Wireless Communications and Mobile Computing*, v. 15, n. 6, p. 1066–1078, 2015. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.2510>.

[43] YANG, Y. et al. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, v. 4, n. 5, p. 1250–1258, 2017.

[44] KIBIRIGE, G. W.; SANGA, C. *A Survey on Detection of Sinkhole Attack in Wireless Sensor Network*. 2015.

[45] PATTON, M. et al. Uninvited connections: A study of vulnerable devices on the internet of things (iot). In: *2014 IEEE Joint Intelligence and Security Informatics Conference*. [S.l.: s.n.], 2014. p. 232–235.

[46] FAGAN, M. et al. *Foundational cybersecurity activities for IoT device manufacturers*. [S.l.]: US Department of Commerce, National Institute of Standards and Technology, 2020.

[47] 42, U. *2020 Unit 42 IoT Threat Report*. `https://unit42.paloaltonetworks.com/iot-threat-report-2020/`. Acessado em: (09/03/2024).

[48] RAZZAQ, M. A. et al. Security issues in the internet of things (iot): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, Science and Information (SAI) Organization Limited, v. 8, n. 6, p. 383, 2017.